

УДК 003.26:51:004(075.8)

Н.Н. Шенец

МНОГОМЕРНОЕ МОДУЛЯРНОЕ РАЗДЕЛЕНИЕ ИНФОРМАЦИИ

Изучается обобщение модулярного разделения информации на многомерный случай. Предлагается алгоритм, реализующий многомерное разделение информации. Построенная схема обладает свойствами однородности и асимптотической идеальности.

Введение

Основы теории разделения информации заложили А. Шамир [1] и Дж. Блейкли [2] в 1979 г. в связи со следующей задачей. Пусть имеются некоторые важные данные s и некоторое множество участников $I = \{1, 2, \dots, t\}$. В качестве данных s может выступать секретный PIN-код или пароль на доступ. По этой причине такую информацию в западной и как следствие отечественной литературе принято называть *секретом*, а само направление в криптографии – *математическим разделением секрета*. В задаче разделения информации требуется так распределить секрет s между участниками I , чтобы лишь заранее определенные (*разрешенные*) подмножества этих участников могли, объединив свои *частичные секреты*, найти истинное значение секрета.

Один из способов решения этой задачи указали М. Миньотт [3], К. Асмус и Дж. Блюм [4]. Его суть состоит в том, что в качестве секрета берется некоторое натуральное число, а частичным секретом i -го участника является наименьший неотрицательный вычет секрета s по некоторому модулю m_i и сам этот модуль. Группа участников может восстановить секрет, лишь решив систему сравнений. Было показано, что путем специального подбора этих параметров можно осуществить *пороговое разделение секрета*, при котором разрешенными подмножествами являются все подмножества заданной или большей мощности. Подход М. Миньотта, К. Асмуса и Дж. Блюма к решению основной задачи называют *модулярным*.

В последнее время модулярное разделение секрета изучали Т. Галибус, Г. Матвеев и Н. Кошур [5–7]. В частности, было установлено, что модулярной реализацией обладает произвольная *структура доступа*, а не только пороговая. Были построены системы модулей для различных структур доступа как в кольце целых чисел, так и в кольцах многочленов над полями Галуа. Последнее особенно важно, так как над кольцами многочленов модулярное разделение секрета обладает наилучшими свойствами по критериям, предложенным в работе [8]. Следует отметить, что алгоритмы разделения информации используются в банковских технологиях (пороговых схемах электронной цифровой подписи) и системах электронного голосования.

Таким образом, модулярное разделение секрета, по крайней мере, над евклидовыми кольцами уже достаточно хорошо изучено. Поэтому логично рассмотреть обобщение полученных результатов на многомерный случай. С этой целью вместо кольца \mathbf{Z} рассмотрим \mathbf{Z} -модуль \mathbf{Z}^n , а вместо модуля участника возьмем подмодуль (подрешетку) [9].

1. Основные определения и обозначения

Дадим сначала формальное определение структуры доступа и, в частности, пороговой структуры доступа.

Определение 1. Под структурой доступа Γ будем понимать любое семейство подмножеств множества всех участников со свойством монотонности, т. е.

$$A \in \Gamma, A \subset B \subset I \Rightarrow B \in \Gamma.$$

Под реализацией структуры доступа Γ будем понимать такой алгоритм, который позволяет восстановить секрет лишь для подмножеств участников, содержащихся в Γ . Если Γ содержит

только все подмножества с мощностью, большей либо равной некоторому k , то такую структуру доступа и соответствующую схему разделения секрета (СРС) называют (k, t) -пороговой.

Воспользуемся некоторыми сведениями из теории решеток [9–10].

Рассмотрим \mathbf{Z} -модуль \mathbf{Z}^n . Пусть $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ – линейно независимые векторы из \mathbf{Z}^n .

Определение 2. Полной решеткой Λ в \mathbf{Z}^n называется множество точек $\left\{ \mathbf{x} = \sum_{i=1}^n u_i \mathbf{a}_i, u_i \in \mathbf{Z} \right\}$, а векторы $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ – ее базисом.

Базис решетки определен неоднозначно. Обозначим через A матрицу, столбцами которой являются векторы \mathbf{a}_i . Будем называть ее базисной матрицей решетки Λ . Любая другая базисная матрица решетки Λ имеет вид $A' = AU$, где U – элемент группы целочисленных матриц с определителем ± 1 . Эту группу принято обозначать через $GL(n, \mathbf{Z})$.

Величина $d(\Lambda) = |\det A| > 0$ не зависит от выбора базиса и называется определителем решетки Λ . Для любой целочисленной решетки Λ существует единственный базис, матрица которого $A = (a_{ij})$ верхнетреугольная с условием $0 \leq a_{ij} < a_{ii}$, $i < j$. Такая матрица называется нормальной формой Эрмита [10].

Нетрудно видеть, что пересечение двух полных целочисленных решеток будет подрешеткой обеих решеток.

Будем также использовать обозначения $(x_1, x_2, \dots, x_n) = \text{НОД}(x_1, x_2, \dots, x_n)$; $[x_1, x_2, \dots, x_n] = \text{НОК}[x_1, x_2, \dots, x_n]$.

2. Многомерные модулярные СРС

Дадим формальное описание многомерной модулярной СРС. В качестве секрета \mathbf{c} выбирается некоторая точка в \mathbf{Z}^n с неотрицательными координатами. Участник СРС получает от дилера некоторый базис целочисленной решетки (матрицу A^i), а также вектор \mathbf{s}^i , выбранный так, чтобы $\mathbf{c} = A^i \mathbf{x}^i + \mathbf{s}^i$ для некоторого $\mathbf{x}^i \in \mathbf{Z}^n$. Для того чтобы определить процедуры разделения и восстановления секрета, необходимо ввести однозначность в выборе базисных матриц A^i и частичных секретов \mathbf{s}^i (будем также называть их *вычетами секрета по модулю подрешетки*).

В качестве базисной матрицы для участника СРС будем использовать верхнетреугольную эрмитову форму. Алгоритм ее вычисления можно найти в работе [10]. Рассмотрим теперь вопрос выбора частичных секретов \mathbf{s}^i . Будем строить их исходя из следующей леммы.

Лемма 1. Пусть задана треугольная базисная матрица A решетки Λ , вектор $\mathbf{c} \in \mathbf{Z}^n$ и числа $k_i \in \mathbf{Z}$, $i = \overline{1, n}$. Тогда существует единственный вектор $\mathbf{s} \in \mathbf{Z}^n$, такой, что

$$1. \quad k_i | a_{ii} | \leq s_i < (k_i + 1) | a_{ii} |, \quad i = \overline{1, n}.$$

$$2. \quad \{A\mathbf{x} + \mathbf{c}, \mathbf{x} \in \mathbf{Z}^n\} = \{A\mathbf{y} + \mathbf{s}, \mathbf{y} \in \mathbf{Z}^n\}.$$

Доказательство. Можно считать, что $a_{ii} > 0$, поскольку для базиса можно использовать и вектор $-\mathbf{a}_i$. Далее утверждение леммы следует из алгоритма деления с остатком, примененного к вектору \mathbf{c} от n -й координаты к первой для верхнетреугольной матрицы или в обратном порядке для нижнетреугольной. ■

Полагая в лемме 1 все k_i равными 0, получаем \mathbf{s}^i с координатами в полуоткрытом параллелепипеде $\{a_{11}^i, a_{22}^i, \dots, a_{nn}^i\}$. Вычисление такого вектора будем называть *приведением вектора \mathbf{s}^i по треугольному базису*.

Теперь опишем процедуру восстановления секрета $\mathbf{c} \in \mathbf{Z}^n$. Пусть имеются два участника СРС с частичными секретами (A^i, \mathbf{s}^i) и (A^j, \mathbf{s}^j) . Секрет принадлежит пересечению множеств

$\{A^i \mathbf{x} + \mathbf{s}^i, \mathbf{x} \in \mathbf{Z}^n\}$ и $\{A^j \mathbf{x} + \mathbf{s}^j, \mathbf{x} \in \mathbf{Z}^n\}$, которое представимо в виде $\{A^{ij} \mathbf{x} + \mathbf{s}^{ij}, \mathbf{x} \in \mathbf{Z}^n\}$, где A^{ij} – базисная матрица пересечения решеток $\{A^i \mathbf{x}, \mathbf{x} \in \mathbf{Z}^n\}$ и $\{A^j \mathbf{x}, \mathbf{x} \in \mathbf{Z}^n\}$, а \mathbf{s}^{ij} – некоторый вектор (это может быть любая точка пересечения). Далее вычисляется эрмитова нормальная форма матрицы A^{ij} и по ней приводится вектор \mathbf{s}^{ij} . Если выполнено условие $c_l < a_{ll}^{ij} \quad \forall l = \overline{1, n}$, то приведенный вектор $\bar{\mathbf{s}}^{ij}$ совпадает с секретом \mathbf{s} . Таким образом, для реализации структуры доступа необходимо и достаточно, чтобы для всех разрешенных подмножеств участников диагональные элементы их общей базисной матрицы были больше соответствующих координат секрета \mathbf{s} , а для остальных (неразрешенных) подмножеств это условие не выполнялось.

Для вычисления базисной матрицы пересечения двух решеток предлагаются два алгоритма. Суть этих алгоритмов состоит в следующем. Пусть заданы две решетки Λ и M в \mathbf{Z}^n с базисными матрицами A и B соответственно. Решаем диофантово уравнение $A\mathbf{x} = B\mathbf{y}$. В результате получаем решение в виде $\mathbf{z} = C\mathbf{q}$, $\mathbf{q} \in \mathbf{Z}^n$, где C – искомая базисная матрица пересечения. Алгоритмы отличаются лишь способом решения диофантова уравнения $A\mathbf{x} = B\mathbf{y}$.

В первом алгоритме от уравнения $A\mathbf{x} = B\mathbf{y}$ переходим к уравнению $\mathbf{x} = A^{-1}B\mathbf{y} = \frac{1}{|A|}L\mathbf{y}$, где

L – целочисленная матрица. Вынесем в правой части диагональную матрицу L^d , на диагонали которой находятся наибольшие общие делители строк матрицы L . Получим уравнение $\mathbf{x} = \frac{1}{|A|}L^d\tilde{L}\mathbf{y}$. Теперь очевидно, что компоненты x_i вектора \mathbf{x} делятся на $\frac{l_{ii}^d}{(|A|, l_{ii}^d)}$ соответствен-

но. Поэтому имеет место представление $\mathbf{x} = H\mathbf{x}'$, где $H = \text{diag}(\frac{l_{ii}^d}{(|A|, l_{ii}^d)}, i = \overline{1, n})$, $\mathbf{x}' \in \mathbf{Z}^n$. Тогда получаем уравнение $|A|\mathbf{x}' = H^{-1}L^d\tilde{L}\mathbf{y}$. Будем искать его решение относительно вектора \mathbf{y} , полагая \mathbf{x}' произвольным. Не ограничивая общности, рассмотрим первую строчку этого уравнения:

$$\tilde{l}_{11}y_1 + \tilde{l}_{12}y_2 + \dots + \tilde{l}_{1n}y_n = c^1x'_1, \text{ где } c^1 = \frac{|A|}{(l_{11}^d, |A|)}, (\tilde{l}_{11}, \tilde{l}_{12}, \dots, \tilde{l}_{1n}) = 1.$$

Используя коэффициенты α_i линейного разложения наибольшего общего делителя чисел \tilde{l}_{1i} , можно найти решение этого уравнения в виде $\mathbf{y} = P_1\mathbf{y}^1$, где элементы матрицы P_1 выражаются через числа α_i , \tilde{l}_{1i} и c^1 , а $y_1^1 = x'_1$. Тем самым обеспечивается делимость первой координаты вектора $L\mathbf{y}$ на $|A|$, причем это будет верным для всех $\mathbf{y}^1 \in \mathbf{Z}^n$. Далее подставляем найденное значение \mathbf{y} в уравнение и повторяем рассуждения для второй строчки. Очевидно, что, последовательно решая диофантовы уравнения, будет найдена матрица C следующим образом:

$$\mathbf{y} = P_1\mathbf{y}^1 = P_1P_2\mathbf{y}^2 = \dots = P_1P_2\dots P_n\mathbf{y}^n \Rightarrow \mathbf{z} = B\mathbf{y} = BP_1P_2\dots P_n\mathbf{y}^n = C\mathbf{y}^n \quad \forall \mathbf{y}^n \in \mathbf{Z}^n,$$

где P_i – матрица решения i -го диофантова уравнения, причем $\det P_i = c^i$, c^i получаются на i -м шаге в результате деления $|A|$ на $(|A|, (l_{i,j}, j = \overline{1, n}))$ (матрица L изменяется после каждой итерации), при этом все $l_{i,j}$ также делятся на их совместный наибольший общий делитель.

Второй алгоритм не использует вычисления обратной матрицы и позволяет решить общую задачу поиска пересечения множеств $\{A\mathbf{x} + \mathbf{s}^1, \mathbf{x} \in \mathbf{Z}^n\}$ и $\{B\mathbf{x} + \mathbf{s}^2, \mathbf{x} \in \mathbf{Z}^n\}$. Диофантово уравнение $A\mathbf{x} = B\mathbf{y}$ решается напрямую. Рассмотрим первое уравнение:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_{11}y_1 + b_{12}y_2 + \dots + b_{1n}y_n = z_1.$$

Обозначим $d_x^1 = (a_{11}, a_{12}, \dots, a_{1n})$, $d_y^1 = (b_{11}, b_{12}, \dots, b_{1n})$. Получим $d_x^1 \alpha^1 = d_y^1 \beta^1 = z_1$, следовательно, $z_1 = [d_x^1, d_y^1] \cdot t_1$. Решаем независимо два уравнения:

$$\bar{a}_{11}x_1 + \dots + \bar{a}_{1n}x_n = c_x^1 t_1;$$

$$\bar{b}_{11}y_1 + \dots + \bar{b}_{1n}y_n = c_y^1 t_1,$$

где $c_x^1 = \frac{[d_x^1, d_y^1]}{d_x^1}$, $c_y^1 = \frac{[d_x^1, d_y^1]}{d_y^1}$.

После этого получим две матрицы $A^1 = AP_1$ и $B^1 = B\tilde{P}_1$, а система примет вид $A^1 \mathbf{x}^1 = B^1 \mathbf{y}^1$, причем $\mathbf{x}_1^1 = \mathbf{y}_1^1$ – общая переменная. Далее решаем все уравнения последовательно и получаем слева и справа одну и ту же базисную матрицу пересечения решеток.

Оба алгоритма имеют сложность $\Theta(n^4)$, поскольку требуется n умножений матриц n -го порядка.

3. Свойства определителя пересечения решеток

Приведем результаты, полученные при исследовании определителя пересечения решеток. Свойства определителя нужны для оценивания качества схем разделения секрета в соответствии с критериями, предложенными в работе [8].

Лемма 2.

1. Пусть Λ и Ω – две решетки в \mathbf{Z}^n . Тогда $d(\Lambda \cap \Omega) = \frac{d(\Lambda) \cdot d(\Omega)}{t}$, где t – некоторый общий делитель $d(\Lambda)$ и $d(\Omega)$.

2. Для любого общего делителя t натуральных чисел a и b существуют решетки Λ и Ω в \mathbf{Z}^n , такие, что $d(\Lambda) = a$, $d(\Omega) = b$, $d(\Lambda \cap \Omega) = \frac{ab}{t}$.

Доказательство. Сначала покажем, что $d(\Lambda \cap \Omega) = [d(\Lambda), d(\Omega)]k$ для некоторого натурального k . Действительно, так как $\Lambda \cap \Omega$ – подрешетка обеих решеток, то $d(\Lambda) \mid d(\Lambda \cap \Omega)$ и $d(\Omega) \mid d(\Lambda \cap \Omega)$ [9].

Теперь покажем, что $d(\Lambda \cap \Omega) \leq d(\Lambda) \cdot d(\Omega)$. Воспользуемся следующим фактом: для любой целочисленной матрицы A существуют такие матрицы $U_1, U_2 \in GL(n, \mathbf{Z})$, что $A = U_1 \cdot \text{diag}(d_1, d_2, \dots, d_n) \cdot U_2$, причем $d_i \mid d_{i+1}$. $A^{-1} = U_2^{-1} \cdot \text{diag}(1/d_1, 1/d_2, \dots, 1/d_n) \cdot U_1^{-1}$ [10].

Поскольку $|U_2^{-1}| = \pm 1$, $|U_1^{-1}| = \pm 1$, то на определитель пересечения влияют лишь числа d_i . Поэтому $d(\Lambda \cap \Omega) = |B| \cdot \prod_{i=1}^n c_i \leq |B| \cdot \prod_{i=1}^n d_i = |B| \cdot |A| = d(\Lambda) \cdot d(\Omega)$, где c_i – числа из первого алгоритма вычисления матрицы пересечения решеток.

Заметим, что можно применить алгоритм нахождения базиса пересечения решеток как к матрице A , так и к матрице B . Имеем $\prod c_i \mid |A|$, $\prod \tilde{c}_i \mid |B|$ (вариант для матрицы B). Можно представить определитель пересечения в виде $d(\Lambda \cap \Omega) = \frac{|A| \cdot |B|}{g} s$, $(g, s) = 1$. Тогда, сравни-

вая две версии алгоритма, получаем $\frac{|A| \cdot |B|}{g_1} s_1 = \frac{|A| \cdot |B|}{g_2} s_2$, причем $\prod c_i = \frac{|A| s_1}{g_1}$, $\prod \tilde{c}_i = \frac{|B| s_2}{g_2}$, следовательно, $g_1 = g_2 \mid (|A|, |B|)$, $s_1 = s_2 = 1$.

Перейдем ко второму утверждению. Рассмотрим (2×2) -матрицы следующего вида:

$$A = \begin{pmatrix} \frac{(a,b)}{t} & 0 \\ 0 & \frac{at}{(a,b)} \end{pmatrix}, \quad B = \text{diag}(1, b).$$

Тогда $d(\Lambda \cap \Omega) = [(a,b)/t, 1] \cdot [at/(a,b), b] = \frac{(a,b)}{t} \cdot [a, b] = \frac{ab}{t}$.

Для произвольного n используем матрицы $\text{diag}(A, E_{n-2})$ и $\text{diag}(B, E_{n-2})$. ■

Следствие. Если $(d(\Lambda), d(\Omega)) = 1$, то $d(\Lambda \cap \Omega) = d(\Lambda) \cdot d(\Omega)$.

Для диагональных базисных матриц A и B решеток Λ и Ω соответственно справедлива формула $d(\Lambda \cap \Omega) = \prod_{i=1}^n [a_{ii}, b_{ii}]$.

Теорема. Пусть A и B – базисные матрицы решеток Λ и Ω соответственно. Для того чтобы $d(\Lambda \cap \Omega) = d(\Lambda) \cdot d(\Omega)$, необходимо, чтобы $((a_{ij}, j = \overline{1, n}), (b_{ij}, j = \overline{1, n})) = 1$, $\forall i = \overline{1, n}$.

Доказательство этой теоремы непосредственно следует из второго алгоритма нахождения базиса пересечения решеток.

4. Произвольная структура доступа

Известно, что в одномерном случае можно реализовать любую структуру доступа модулярной СРС [6]. Покажем, что и в многомерном варианте это возможно.

Лемма 3. Пусть A и B – две базисные матрицы, а C – матрица пересечения соответствующих решеток. Тогда для любой невырожденной матрицы U матрица пересечения решеток $\{UA\mathbf{x}, \mathbf{x} \in \mathbf{Z}^n\}$ и $\{UB\mathbf{x}, \mathbf{x} \in \mathbf{Z}^n\}$ имеет вид UC .

Доказательство непосредственно следует из первого алгоритма нахождения матрицы пересечения решеток:

$$\mathbf{x} = (UA)^{-1}UB\mathbf{y} = A^{-1}B\mathbf{y} \Rightarrow \mathbf{z} = UB P_1 P_2 \dots P_n \mathbf{y}^n \cong UC\mathbf{t}.$$

Пусть имеется n одномерных модулярных реализаций структуры доступа Γ . Составим из модулей участников диагональные матрицы и домножим каждую слева на верхнетреугольную унимодулярную. Тогда эти матрицы позволяют реализовать Γ в многомерном случае, причем это не будет прямым произведением одномерных схем.

Получено также и более интересное утверждение. Оказывается, в многомерном варианте можно реализовать произвольную структуру доступа при попарно взаимно простых определителях подрешеток участников.

5. Однородные (k, t) -пороговые модулярные СРС

Рассмотрим (k, t) -пороговые схемы специального вида. Речь здесь идет об аналоге схемы Асмуса–Блюма в многомерном случае. Рассмотрим сначала одномерную схему. Пусть в качестве модулей выбраны простые числа $p_0 < p_1 < \dots < p_t$, секрет выбирается из \mathbf{Z}_{p_0} . Генериру-

ются числа $r_1 \in \mathbf{Z}_{p_1}, r_2 \in \mathbf{Z}_{p_2}, \dots, r_{k-1} \in \mathbf{Z}_{p_{k-1}}$ и ищется $Y \in \mathbf{Z}_P$, где $P = \prod_{i=0}^{k-1} p_i$ и $Y \equiv r_i \pmod{p_i}$. Да-

лее вычисляются частичные секреты для участников: $s_i = Y \pmod{p_i}$. В работе [8] показано, что такая схема при последовательных простых модулях асимптотически идеальна.

Рассмотрим многомерный аналог этой схемы, основанный на одномерной схеме. Пусть $n = t$ и на диагоналях базисных матриц участников расположены простые числа p_i , $i = \overline{1, t}$, причем так, чтобы у всех участников на одной и той же позиции находились разные числа (это можно сделать, например, циклическим сдвигом). Наддиагональные элементы заполним произвольным образом. Возьмем n секретов из \mathbf{Z}_{p_0} и используем их в качестве координат вектора-

секрета. Отметим, что определители подрешеток участников одинаковы и равны $\prod_{i=1}^n p_i$, по-

этому множества выбора частичных секретов участников равномогущны. Такие схемы называют *однородными*. Получим оценку для падения энтропии такой схемы, аналогичную оценке из [8].

Лемма 4. Пусть вектор-секрет равномерно распределен в $\mathbf{Z}_{p_0}^n$. Тогда

$$\Delta_c(\mathbf{s}^i : i \in \tilde{I}) \leq \sum_{j=1}^n \log \left(\frac{p_0 (\lfloor (C(\tilde{I}_j) + 1) / p_0 \rfloor + 1)}{C(\tilde{I}_j)} \right), \text{ если } |\tilde{I}| < k,$$

и $\Delta_c(\mathbf{s}^i : i \in \tilde{I}) = n \log p_0$ в противном случае. Здесь \tilde{I}_j – множество участников одномерной модулярной СРС, которому соответствуют модули в (j, j) -х координатах базисных матриц участников из множества \tilde{I} ,

$$C^*(\tilde{I}) = \left(\prod_{i=0}^{k-1} p_i \right) / \left(\prod_{v \in \tilde{I}} p_v \right), \quad C(\tilde{I}) = \lfloor C^*(\tilde{I}) \rfloor.$$

Доказательство. В случае $|\tilde{I}| \geq k$ секрет однозначно восстанавливается, поэтому для условной энтропии выполняется условие

$$H(\mathbf{c} \in \mathbf{Z}_{p_0}^n \mid \mathbf{s}^i : i \in \tilde{I}) = 0 \Rightarrow \Delta_c(\mathbf{s}^i : i \in \tilde{I}) = H(\mathbf{c} \in \mathbf{Z}_{p_0}^n) - H(\mathbf{c} \in \mathbf{Z}_{p_0}^n \mid \mathbf{s}^i : i \in \tilde{I}) = n \log p_0.$$

Пусть теперь $|\tilde{I}| < k$. Обозначим через V множество точек из \mathbf{Z}_P^n , где $P = \prod_{i=0}^{k-1} p_i$, которые лежат в пересечении множеств участников. Базисная матрица их пересечения на диагонали содержит произведения соответствующих диагональных элементов матриц участников, т. е. $a_{ii}^{\tilde{I}} = \prod_{v \in \tilde{I}} a_{ii}^v$. Тогда согласно лемме 1 минимальное число точек в V будет равно

$$\prod_{j=1}^n \left\lfloor P / a_{jj}^{\tilde{I}} \right\rfloor = \prod_{j=1}^n C(\tilde{I}_j).$$

Для определения максимального числа точек из V , приведение которых по диагональной матрице $\text{diag}(p_0, p_0, \dots, p_0)$ дает в точности фиксированный вектор $\mathbf{s} \in \mathbf{Z}_{p_0}^n$, рассмотрим пересечение множеств $\{A^{\tilde{I}} \mathbf{x} + \mathbf{s}^{\tilde{I}}, \mathbf{x} \in \mathbf{Z}^n\}$ и $\{\text{diag}(p_0, \dots, p_0) \cdot \mathbf{x} + \mathbf{s}, \mathbf{x} \in \mathbf{Z}^n\}$. Поскольку p_0 взаимно просто с диагональными элементами $a_{ii}^{\tilde{I}}$, то такое пересечение не пусто и матрица пересечения на

диагонали имеет элементы $a_{ii}^j p_0$. Тогда опять же по лемме 1 максимальное число точек в V , дающих фиксированный вектор $\mathbf{s} \in \mathbf{Z}_{p_0}^n$, будет $\prod_{i=1}^n \left\lceil P / p_0 a_{ii}^j \right\rceil \leq \prod_{i=1}^n (\lfloor (C(\tilde{I}_i) + 1) / p_0 \rfloor + 1)$. Поэтому

$$P(\mathbf{c} = \mathbf{s} \mid \mathbf{s}^i : i \in \tilde{I}) \leq \frac{\prod_{i=1}^n (\lfloor (C(\tilde{I}_i) + 1) / p_0 \rfloor + 1)}{\prod_{i=1}^n C(\tilde{I}_i)} = \prod_{i=1}^n \frac{(\lfloor (C(\tilde{I}_i) + 1) / p_0 \rfloor + 1)}{C(\tilde{I}_i)},$$

и тогда по определению $H(\mathbf{c} = \mathbf{s} \mid \mathbf{s}^i : i \in \tilde{I}) \geq -\log P(\mathbf{c} = \mathbf{s} \mid \mathbf{s}^i : i \in \tilde{I})$. Отсюда получаем требуемую оценку. ■

В работе [8] доказательство асимптотической идеальности основано на использовании оценки падения энтропии, которая соответствует слагаемым в оценке из леммы 3, и показано, что каждое такое слагаемое стремится к нулю, а значит, и сама сумма также будет стремиться к нулю при росте p_0 . Следовательно, предлагаемый многомерный аналог будет асимптотически совершенной модулярной СРС. В работе [8] также показано, что $p_j / p_0 \rightarrow 1$ при $p_0 \rightarrow \infty$. Это соответствует асимптотической идеальности. В рассмотренном выше случае никаких существенных отличий нет, поэтому схема также будет асимптотически идеальной. Отметим, что, в отличие от одномерной схемы, эта схема является и однородной.

Заключение

В работе предложена схема многомерного модулярного разделения секрета. Подобные исследования, насколько известно автору, проведены впервые. В частности, решена задача построения СРС, а именно предложены два алгоритма нахождения базисной матрицы пересечения подрешеток и общего вектора-вычета, алгоритмы построения эрмитова базиса и приведения секрета по модулю подрешетки. Предложен способ реализации произвольной структуры доступа и однородной пороговой схемы доступа. Доказана также асимптотическая идеальность однородной пороговой схемы Асмуса–Блюма, основанной на последовательных простых числах.

К числу преимуществ многомерных схем можно отнести большой выбор параметров и возможность строить однородные схемы, однако при этом возрастает сложность алгоритма восстановления секрета, хотя она остается полиномиальной. Заметим также, что все свойства одномерных модулярных СРС с помощью леммы 1 могут быть перенесены и на многомерный случай.

Список литературы

1. Shamir, A. How to share a secret / A. Shamir // Communications of the ACM. – 1979. – Vol. 22 (1). – P. 612–613.
2. Blakley, G.R. Safeguarding cryptographic keys / G.R. Blakley // Proc. of the AFIPS National Computer Conference. – New York, 1979. – Vol. 48. – P. 313–317.
3. Mignotte, M. How to share a secret / M. Mignotte // Advances in Cryptology – Eurocrypt’82, LNCS. – 1982. – Vol. 149 – P. 371–375.
4. Asmuth, C. A modular approach to key safeguarding / C. Asmuth, J. Bloom // IEEE Transactions of Information Theory. – March 1983. – Vol. 29. – P. 208–210.
5. Galibus, T. Mignotte’s sequences over polynomial rings / T. Galibus, G. Matveev // Proc. International Workshop on Information and Computer Security. – Timisoara, Romania, 2006. – P. 39–44.
6. Галибус, Т.В. Разделение секрета над полиномиальными кольцами / Т.В. Галибус // Вестник БГУ. – 2006. – Сер. 1, вып. 2. – С. 97–100.

7. Кошур, Н.Н. Генерация модулей для пороговых схем / Н.Н. Кошур, Г.В. Матвеев // Вопросы информационной безопасности: сб. науч. тр. – Минск, 2002. – Вып. 1 – С. 85–88.
8. Quisquater, M. On the security of the threshold scheme based on the chinese remainder theorem / M. Quisquater, B. Preneel, J. Vandewalle // Lecture Notes in Computer Science. – 2002. – Vol. 2274. – P. 199–210.
9. Касселс, Дж. Введение в геометрию чисел / Дж. Касселс. – М.: Мир, 1965. – 424 с.
10. Cohen, H. A course in computational algebraic number theory / H. Cohen. – Berlin: Springer-Verlag, 1993. – 545 p.

Поступила 26.03.07

*Белорусский государственный университет,
Минск, пр. Независимости, 4
e-mail: Shenets_n_1984@tut.by*

N.N. Shenets

MULTIDIMENSIONAL MODULAR SECRET SHARING

A multidimensional variant of modular secret sharing is studied. The algorithms for realization of such schemes are proposed. The asymptotically ideal homogeneous threshold multidimensional modular secret sharing scheme is constructed.